Credentialing Project Technical Architecture

Presented to

Transportation Industry Association

Stakeholder Meetings

April 11-29, 2002

Agenda

- Overview of High Level Architecture Vision
- Components of Architecture
  - Technical
  - Business Process
- Key Issues
- Discussion

TSA Mission and Vision

TSA Mission

To protect the nation's transportation systems to ensure freedom of movement for people and commerce.

TSA Vision

TSA will continuously set the standard for excellence in transportation security through its people, processes and technologies

Industry Association Tentative Schedule

Stakeholder Category	Proposed Dates	Time and Location
Maritime	April 11, 2002	10:00 – 3:00, Room 2201, Nassif Building, US Department of Transportation, 400 Seventh Street, SW, Washington, DC
Aviation	April 12, 2002	10:00 – 3:00, Room 6200, Nassif Building, US Department of Transportation, 400 Seventh Street ,SW, Washington, DC
Transit	April 16, 2002	10:00 – 3:00, Room 4200, Nassif Building, US Department of Transportation, 400 Seventh Street, SW, Washington, DC
Other Surface	April 18, 2002	10:00 – 3:00, Room 4200, Nassif Building, US Department of Transportation, 400 Seventh Street, SW, Washington, DC

Tentative Agenda

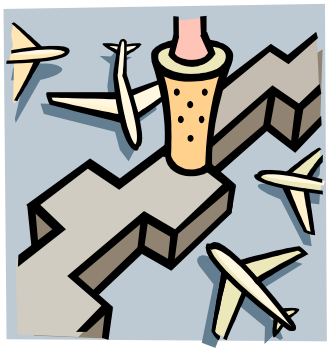
Time	Topic	Presenter
10:00 – 10:30	Introduction	Chris McMahon, Special Assistant to the Secretary, Pat Schambach, TSA CTO/CIO, and Gregg Hawrylko, Credential Project Lead
10:30 – 12:30	Present Overall Credential System Architecture	Jack Cassidy, TSA Credential Project , and Phill Loranger, FAA Chief, Access Enabling Technologies
12:30 – 1:30	Lunch and Informal Discussions	Jack Cassidy and Phill Loranger
1:30 – 2:30	Discuss Issues with Participants	Jim Zok, Chairman CDAG and MARAD Associate Administrator
2:30 – 2:55	Overview Cost Sharing Options	Jack Cassidy
2:55 – 3:00	Summary and Next Steps	Jim Zok and Jack Cassidy

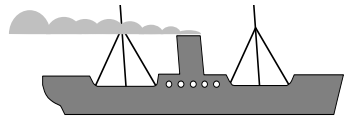
Review

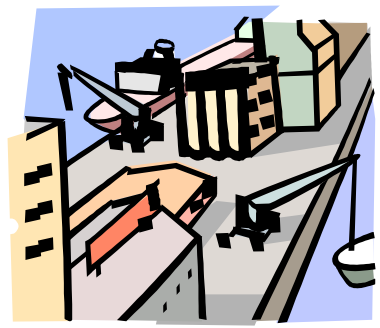
- **Vision: Establish the transportation system-wide common architecture to meet current and future, physical and logical access, and privacy requirements for all personnel, of all transportation modes.**

- **Primary focus: "transportation workers"- any person who requires unescorted access to a secure area of the transportation system.**
  - **Goals:**
    - **One standardized credential.**
    - **One integrated and secure network of databases.**
  - **Key Principles:**
    - **Leverage the current local authority/agency and industry investments**
    - **DOT defines minimum security and privacy requirements, technology standards, certification and performance requirements**
    - **DOT provides guidance and incentives to local authorities for technology refreshment and investment decisions to enhance migration to increased use of common credential platform**
    - **DOT fields the common credential and issuance infrastructure**
    - **Balance security, commerce and privacy requirements**
    - **Maximum use of outsourcing**
    - **Public-Public-Private Partnership**

Goals

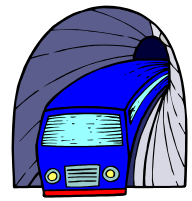


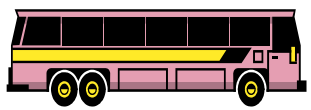


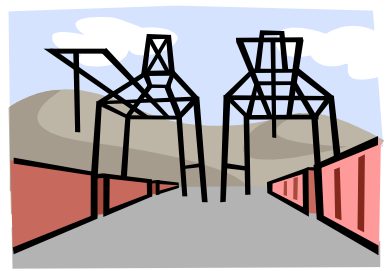


One standardized credential

- Universally recognized and accepted across the DOT
- Able to be used locally within the facility infrastructure
- Meets multiple levels of secure access requirements.



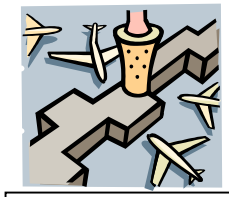




Goals

One integrated & secure network of databases

- Leverages current local database infrastructure
- Includes all enrolled personnel
- Reference Biometric



Perimeter Access Station

Security Access Station

Security Access Station

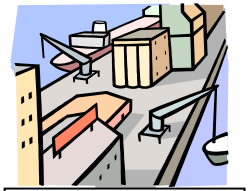
LA

TWIC Data Base and Issuance Center

TSA
Central Control Point

FBI, INS, Federal Systems

VPN



Perimeter Access Station

Security Access Station

Security Access Station

Miami

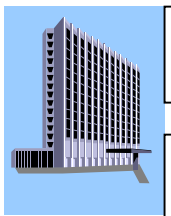
TWIC Data Base and Issuance Center

Perimeter Access Station

Security Access Station

Security Access Station

HQ



TWIC Data Base and Issuance Center

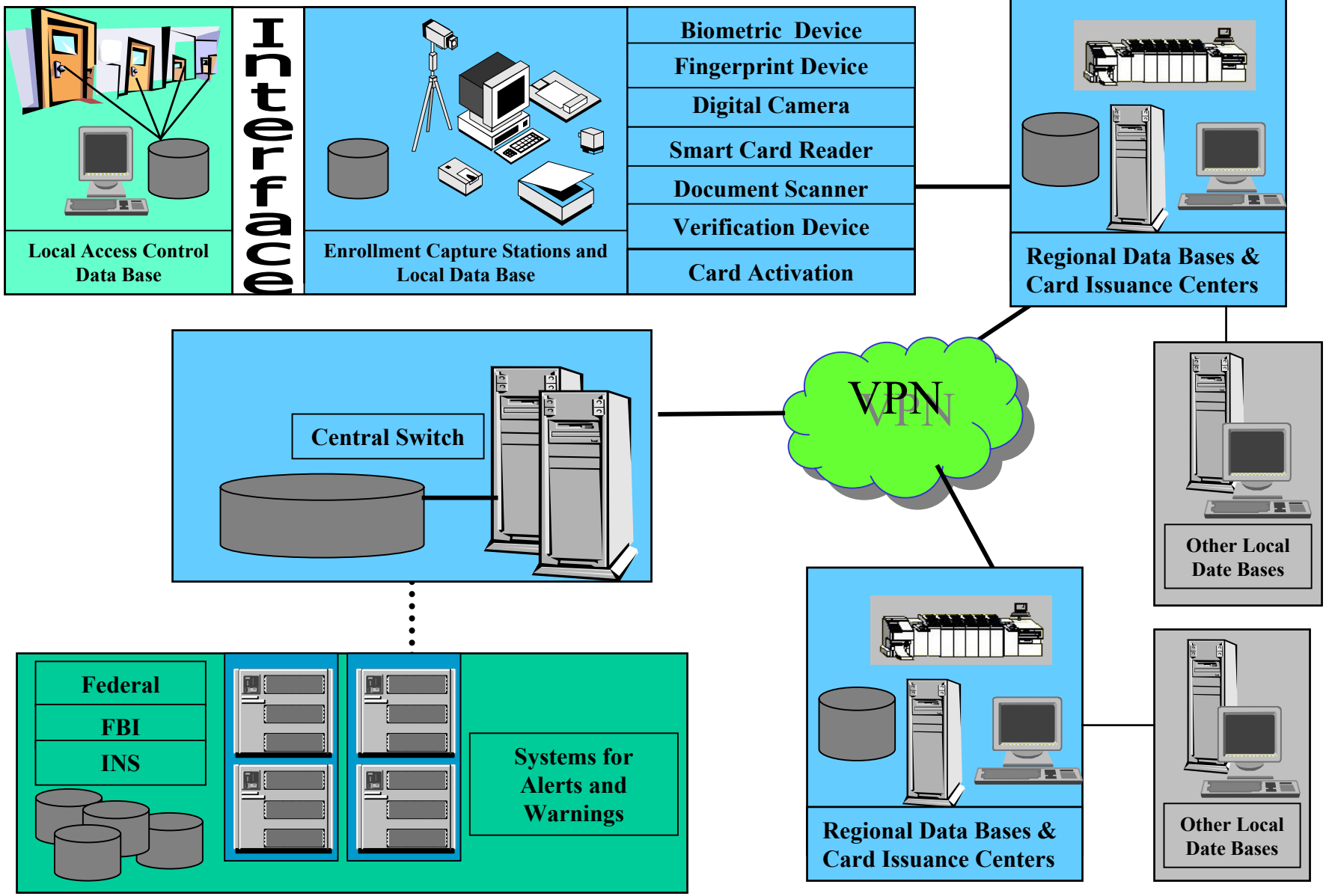
Perimeter Access Station

Security Access Station

Security Access Station

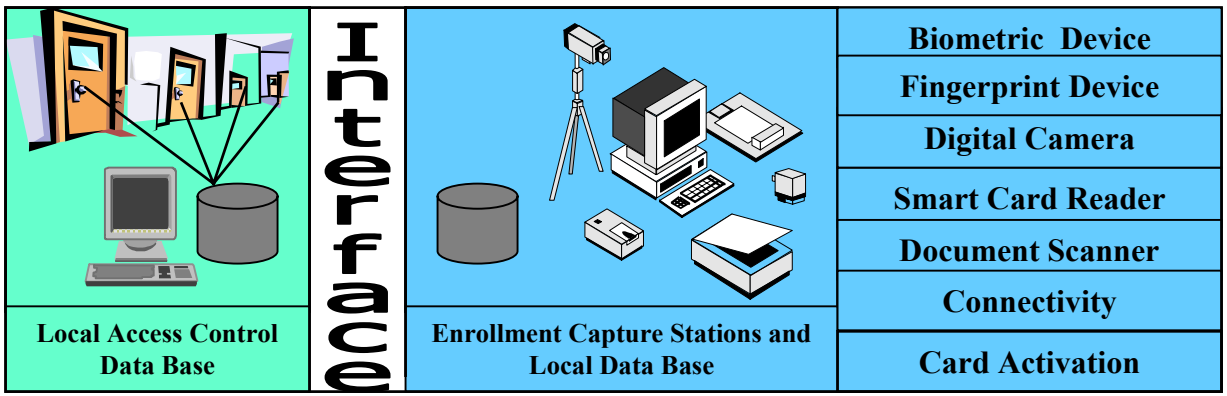
Chicago

Major Components



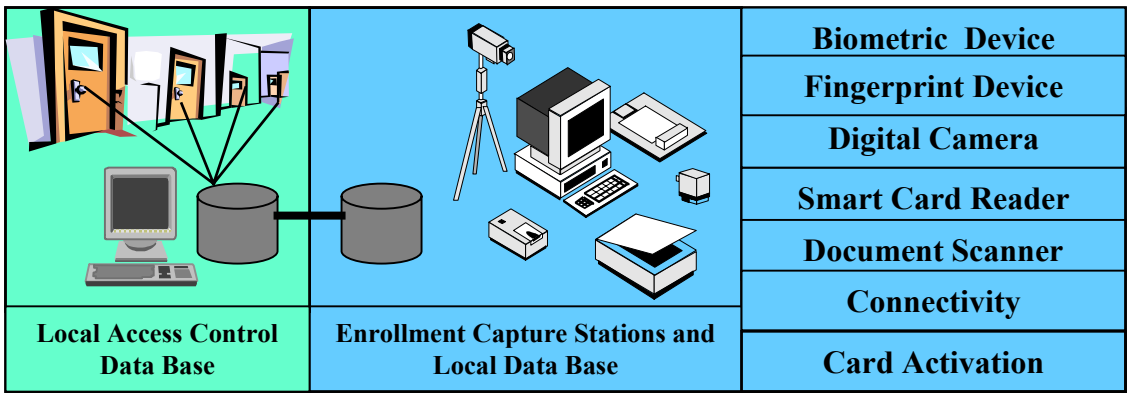
Local Card System/TSA EC Sub-System

The 1st scenario depicts a local facility with a closed local system and the TSA Enrollment/Capture systems co-located, but with a low level of system integration. The local facility has not begun to utilize the TWIC technologies in the local access control system. Transportation workers are enrolled in the TWIC system, but only those who travel to other locations will have direct use of TWIC. This configuration is less desirable because of the disconnected systems approach.



TSA Capture and Enrollment Module

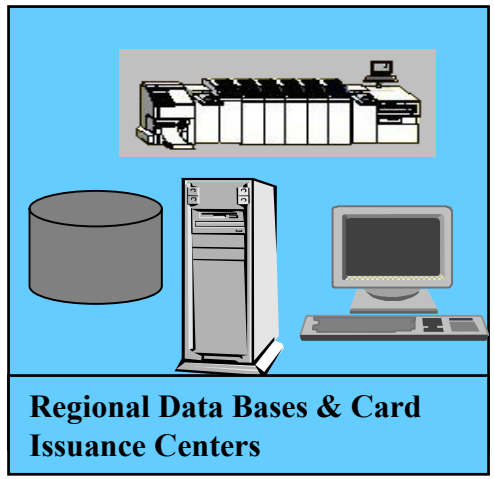
The 2nd scenario depicts a local facility that has elected to use the TSA Enrollment/Capture system as an integrated solution. TW are issued and use TWIC based technology in local facility and those TW who are mobile have TWIC available for use. This configuration is most desirable because of the simplified systems approach.



Regional Data Bases

• Regional processing centers are clustered server sites with a storage area network array and high capacity TWIC initialization and personalization (printing, loading) capability.

•This site hosts the web enabled application program and the relational database server required to warehouse the appropriate data collected by local facilities and issue large number of cards with high quality printing.



Regional Data Bases & Card Issuance Centers

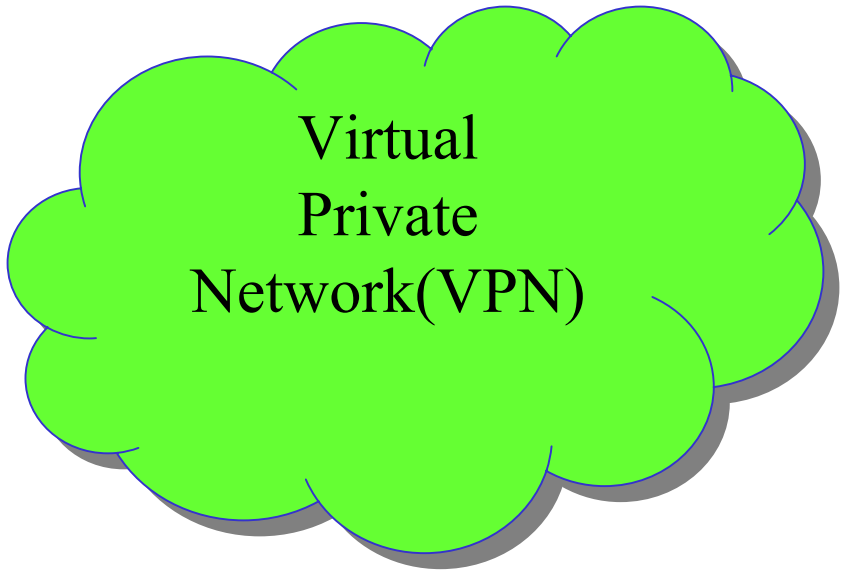
•The data maintained here could be the complete enrollment record for each TWIC holder within the region. All orders for TWIC cards will be processed and shipped to the local enrollment and capture station for final verification and issuance to the TW.

Virtual Private Network

The network component is either an existing public (Internet), or a private communications network available across wide geographic areas or a combination of the two. It could also leverage the existing State DOT's networks combined with the Internet.

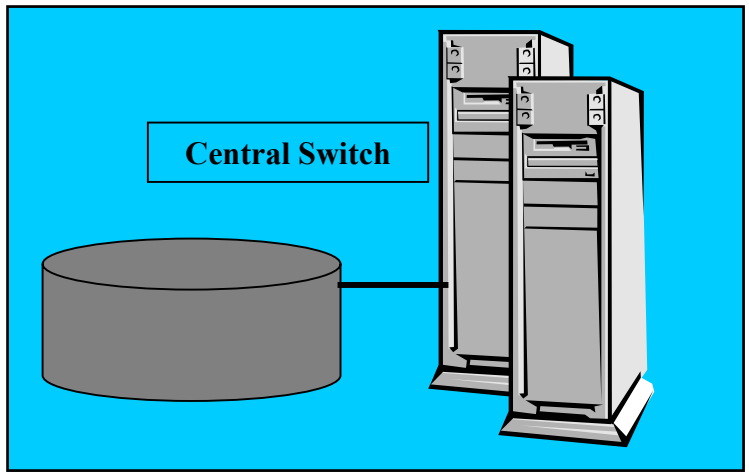
It will be made secure by implementing an encryption system utilizing the TWIC as a token to carry PKI certificates and/or hard IPSEC tunnels.

Depending on the size of a local facility, the network must accommodate the full range of communication capability, including traditional dial-up, ISDN, DSL, Cable, wireless and Leased lines.



TSA Central Switch

The Central switch is a clustered server site with a storage area network array. It will host the web enabled application program and the relational database servers.



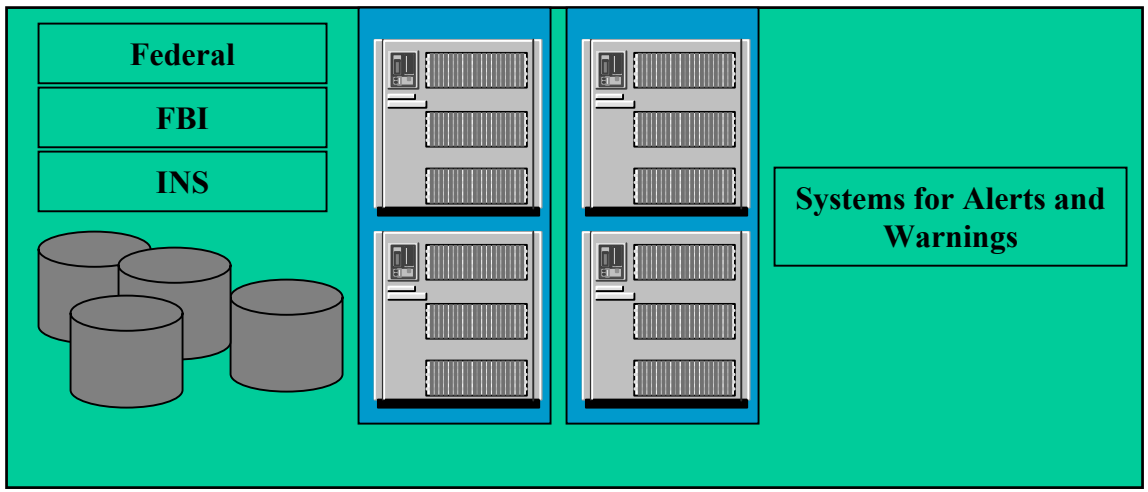
The data records are limited to a minimum number of elements including:

- **TWIC identity record number**
- **Claimed Identity (name)**
- **Reference Biometric**
- **Clearance Access Level Granted**
- **Locations currently granted access**
- **Control flags, and other pointers**
- **Card Number(s) actively assigned to record**

TSA Central will be the control point for card management (e.g. hot lists, verifications) and to interface with other intelligence, threat and warning systems

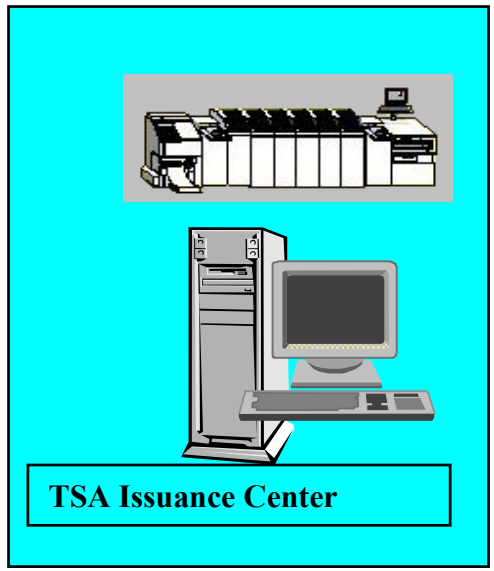
Affiliate Organizations/Processes

Many other organizations and systems are available via the network. These systems can be part of the authentication process or integrated into the National Threat Alert System. These connections are to the TSA Central Switch and information is broadcast to the Regional and Local facilities via the Command and Control Notification subsystem.



TSA Card Issuance Center

The TSA Card Issuance Centers will be either co-located with Regional Centers or stand alone sites that process card personalization requests. The cards are initialized and personalized in accordance with the enrollment request form, PKI certificates loaded under controlled conditions, card electronically locked and shipped/transferred securely to the designated issuance point.



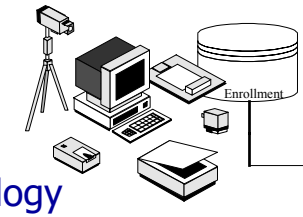
Benefits:

- **Secure Card Life Cycle**
- **High Security/Quality Printing**
- **Economic Scale in card stock and printing**
- **High Volume PKI Certificate generation and loading**
- **Reduced billets and training requirements**

Card Architecture

Standards Based Solution

- GSA Smart Card Interoperability Schedule
  - Leverage inherent strength of smart card technology
  - Standard Data Model for the DOT Container
  - Established Standards, Specifications, Performance
  - Multiple Vendor Sources
    - Use 'Market Force' for validation of 'new' technology
  - Commercial Technology Based Infrastructure
    - COTS
    - FIPS 140 Compliant
- Expected Standards for the Smart Card Technology
  - GSA Interoperability Specification GSA-IS
  - 32K EEPROM (ICC) migrating to 64K
  - JAVA OS Open Platform
  - Contact chip migrating to Contact-Contact-less capability
  - Additional technologies (barcodes, magnetic stripe) may be implemented based on Agency and Stakeholder requirements
  - Supports integration with current infrastructure investment



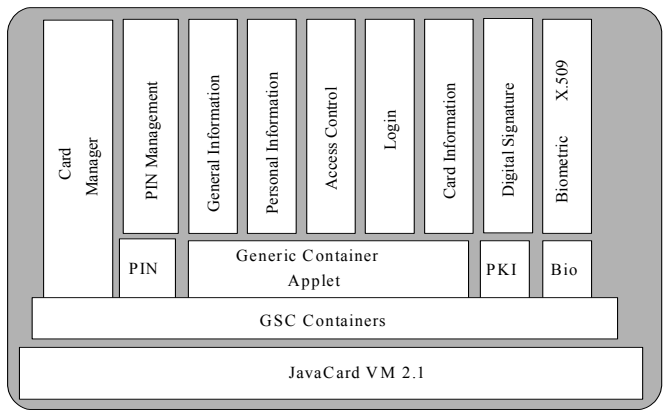
Enrollment Station

ISO Standards

Interoperable with GSA

FIPS 140 Level 2 Secure

JAVA 32K EEPROM



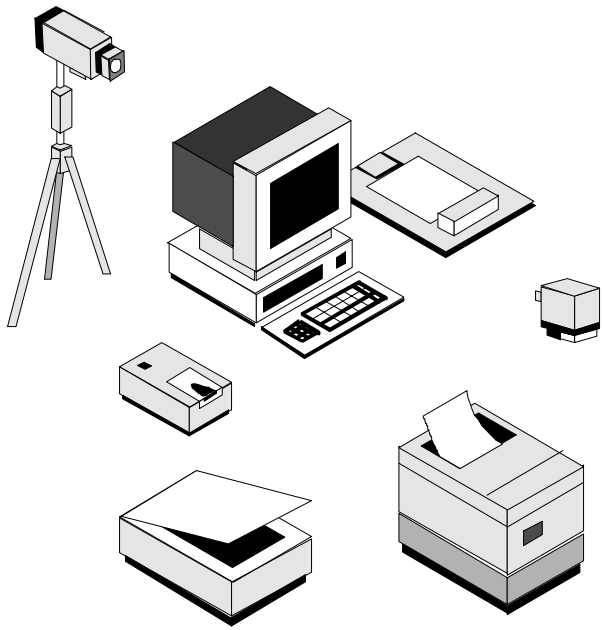
TSA Standard Enrollment and Capture Workstations

Digital Camera

Biometric Capture Device

Document Scanner

Document Authentication



Enrollment Request & Enrollment Record

Fingerprint Device 10 print (Fingerprint Scanner)

Smart Card Reader

Card Activation and Verification

Local Data Base

Background Check Requirements

Regional Data Base

Central Data Switch

Documentation Requirements for Claimed Identity

- Verification of Claimed Identity is weak link for all Credential Systems

- TWIC working group is investigating a system with multiple categories of documents that may include:
  - Government issued picture identification card
  - Other government issued identification card
  - Documentation of a link to a local community
  - Documentation of employment from known employer

Enrollment and Issuance

Simplified Process for Enrollment and Issuance of TWIC

Enrollment and Capture Station

Claimed Identity Documentation → Background Check Fingerprints, Drug Test etc → DOT "57" Data Capture → Digital Photo & Biometric Capture

Business Hours

Central and Other Agencies

Central Establishes Reference Completes 1:N Biometric Search

Background Check Process—Fingerprint etc Completed by other Agencies

Overnight

Enrollment and Capture Station

Compile Responses & Decision to Issue → Regional Printer Card Initialization and Final Personalization → Notify Central and Individual

Overnight

Enrollment and Capture Station

Unlock card, Conduct Biometric 1:1 Check Worker-Enrollment Request-Card → Validate Data, Notify Central → Issue Card

Business Hours

Enrollment and Issuance

Integration of Process

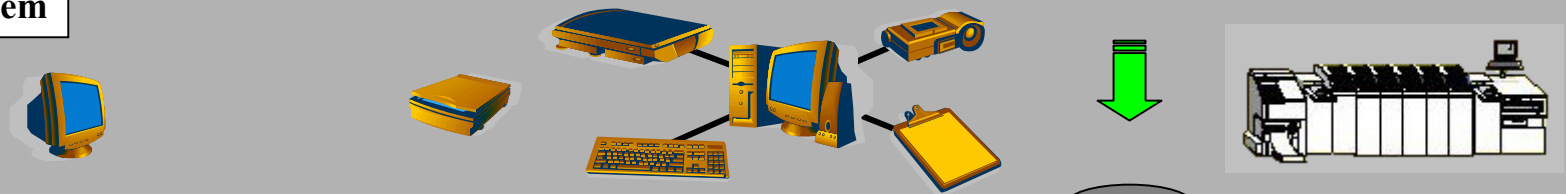
TWIC Process

- Employer Requests TWIC
- Review & Accept Documents
- Other Agencies and Central for 1:N Match
- Decision Process
- Card Initialization and Personalization

Worker

- Worker presents Required Documents:
  - •Photo Identity Card
  - •Birth Certificate
  - •Link to Community
  - •Link to Employer
- Background Check Data:
  - Fingerprints
  - Drug Test
  - etc
- Build Enrollment Record
  - DOT "57"
  - Digital Photo
  - Reference Biometric
- Validate Reference Biometric and Receive Card

System



- Screens flows
- Data and Biometric Capture
- Data Transfer
- Card Personalization

Activation Phase

Simplified Process for Activation of the TWIC

Enrollment and Capture Station

Claimed Identity & Present TWIC → Verify Biometric 1:1 Match → Review Access Level and Access Request → Grant Appropriate Access

Business Hours

Local Access System

If not TWIC Compatible, Grant Access and Issue Device

If TWIC Compatible, Grant Access And Use TWIC

Business Hours

Enrollment and Capture Station

Notify Central of Access Level Granted

Business Hours

Revocation Phase

Simplified Process for Revocation of the TWIC

Enrollment and Capture Station

Revocation Request → Verify Request

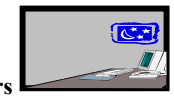
Business Hours

Overnight

Local Access System

TW and TWIC are deactivated in local system

Business Hours



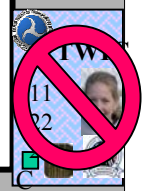
Overnight

Business Hours

Enrollment and Capture Station

Notify Central
- Add to National Hot List
- Notify listed locations to positively revoke access

If TWIC physically presented or use is attempted, it fails. When obtain custody of card, notify Central to remove from Hot List



Overnight

Business Hours

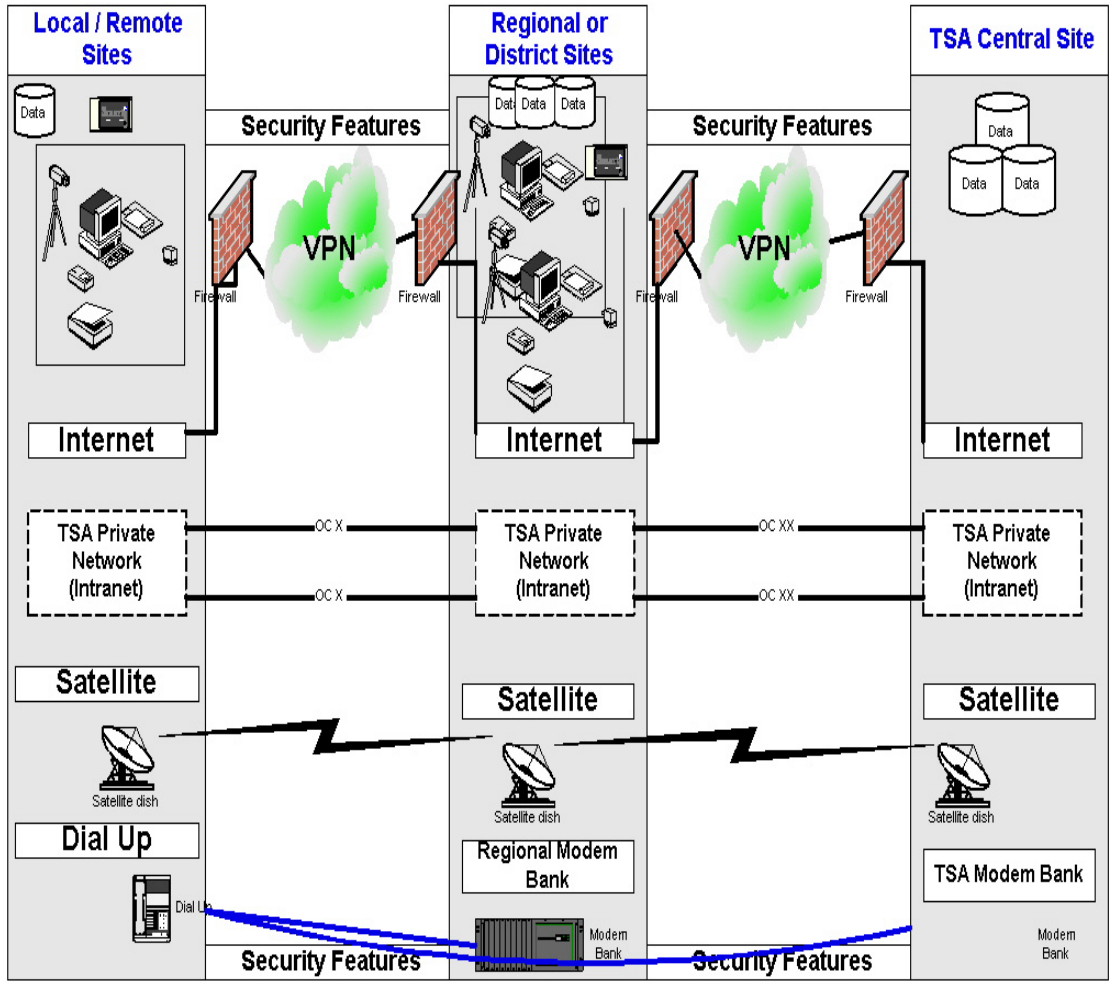
Local Access System

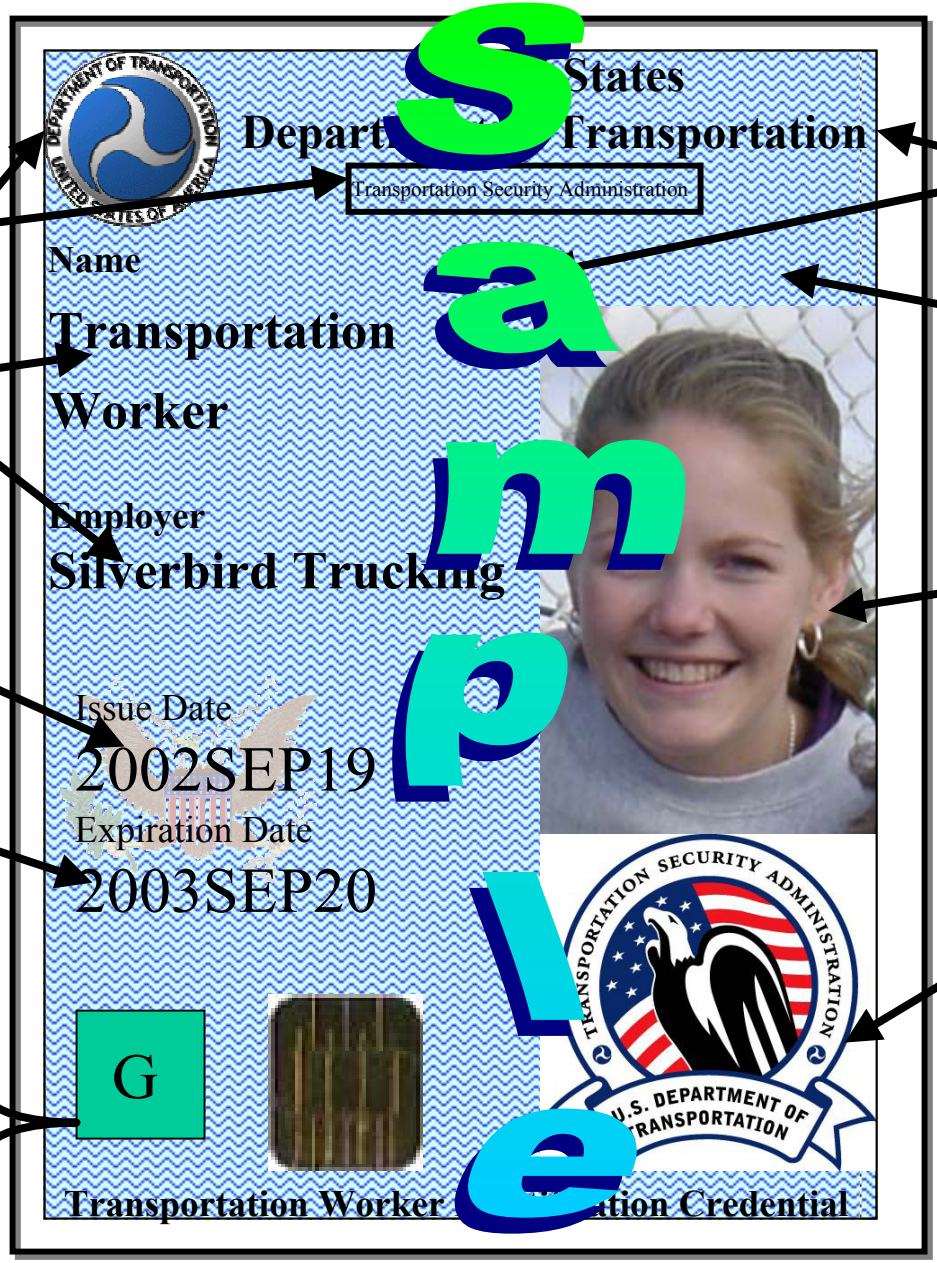
Local and Central archive the record information.

Overnight

Communications for Credentials

- **Task: Integration with 1000+ local sites with varying database and communications suites**
- **Regional sites must be able to support full range of local communication capability from sophisticated to basic.**
- **TSA Central must also be able to support the full range.**
- **Security features may be pre-existent and require integration into other TSA networks, or need to be developed.**




Micro Printing Technology
Variable Printed Data
Optical Variable Devices
Ultraviolet Ink
G C L
Government Employee Contractor and LEO
.5mm Overlay for ink protection
Guilloche Pattern
High Resolution Digital Photo
Crest of Logo of home or host agency or group
States
Transportation
Transportation Security Administration
Name
Transportation Worker
Employer
Silverbird Trucking
Issue Date
2002SEP19
Expiration Date
2003SEP20
G
Transportation Worker
Credential
SAMPLE


Triple
Track
Ghost
Image
This card is property of the DOT, and is intended fo ial identif
purposes only ,and misuse, alteration or a bj Title 18 U 99 50
and 701. If found mail to DOT, 400 W C rn Postage
Guaranteed.
SAMPLE
2D Barcode
TWIC Card # for
card management
and alternative
hot list
T Card #
OR 44
ss earance Level
2
Dimple
opposite
chip cavity
Transportation Security Administration
Property of the US Government
SWIG Specification
Access Level
Variable Optical
Devices

-

Discussion Items

Examples of Policy Issues

- Request for TWIC—from Employer, pre-post employment
- Cost Sharing—Local Tradition, Value-Benefit Determined etc
- Privacy—Records, Location, Records Retention etc
- Access Levels—Map to standard categories, specific requirements
- Results of Background Investigation—Access, Appeal, Retention
- Claimed Identity Documentation—Categories, Number of Documents
- Appeal Process at all decision points in process

Next Steps

Credential Project Office and Composite GT51-CDAG Group will:

- Complete the series of Industry Association Meetings
- Use our multi-modal working groups to finalize key components and issues:
  - Topology Design (Visual Appearance, Printed Information and Technology Layout)
  - Claimed Identity Documentation
  - Specific requirements (Recommended Pilots, Additional Technology, Populations)
  - Policy Issues
  - Cost Sharing Detailed Strategy
- Continue to improve our engagement with the full range of stakeholders and channel feedback to improve and field the vision in Public-Public-Private Partnership
- Prepare for the June Pilot Phase